Integrating Strategic Information Security with Strategic Information Systems Planning (SISP)

Md Hafiz Selamat[α], Mohd Adam Suhaimi[β], Husnayati Hussin[γ]

[α]*Faculty of Computer Science and Information Systems*
Universiti Teknologi Malaysia, Skudai, Johor.
E-mail: hafiz@fsksm.utm.my

[βγ]*Kulliyah of Information Communication Technology*
International Islamic Univeristy Malaysia, Gombak, Selangor
E-mail: [β]adam@iiu.edu.my; [γ]husnayati@iiu.edu.my

ABSTRACT

Strategic information systems planning and strategic information security are two different atributes in information systems world. Information systems security must be integrated with business plan (Wylder, 2003) and strategic information systems planning must be align with business plan. This study aims to investigate the contribution of information security attributes to the strategic information systems planning in the organization. Strategic information system planning (SISP) is an exercise or ongoing activities that enable organization to develop priorities for information system (IS) development (Doherty, 1999). SISP approach is a combination of method, process and implementation (Earl, 1993). As a new business strategies and information technologies are both rapidly moving targets, it is a very challenging task to produce an effective plan that achieves business objectives with efficient information systems support (Hevner et al. 2000). Organization invest very large amount of time and money in the SISP project. In a typical SISP project, term of key managers, users, selected clients, and IS specialist are formed (Hevner et al. 2000) and planning methodology is chosen. On the other hand, Information security planning is to mitigate risk associated with the processing of information with confidentially, integrity and authenticity (Wylder, 2003). Finally, this study will introduce a new model of SISP embedded with information security attributes based on previous literature on both SISP and strategic information security.

Keywords: *strategic information systems planning, strategic information security; information systems security*

1.0 Introduction

Planning for information systems, as for any other system, begins with the identification of organizational needs. In order to be effective, development of any type of computer-based system should be a response to need-whether at the transaction processing level or at the more complex information and support systems levels. Such planning for information systems is much like strategic planning in management. Objectives, priorities, and authorization for information systems projects need to be formalized. The systems development plan should identify specific projects slated for the future, priorities for each project and for resources, general procedures, and constraints for each application area. The plan must be specific enough to enable understanding of each application and to know where it stands in the order of development. Also the plan should be flexible so that priorities can be adjusted if necessary. King (King, 1995) in his recent article has argued, strategic capability architecture - a flexible and continuously improving infrastructure of organizational capabilities – is the primary basis for a company's sustainable competitive advantage. He has emphasized the need for continuously updating and improving the strategic capabilities architecture.

Relationship between information system functions and corporate strategy was not of much interest to Top Management of firms. Information Systems were thought to be synonymous with corporate data processing and treated as some back-room operation in support of day-to-day mundane tasks (Rockart, 1979). In the 80’s and 90’s, however, there has been a growing realization of the need to make information systems of strategic importance to an organization. Consequently, strategic information systems planning (SISP) is a critical issue. In many industry surveys, improved SISP is often mentioned as the most serious challenge facing IS managers.

Organizations nowadays depend largely on computer based Information Systems (IS) for a vital part of their operation. IS comprise the information that is being stored, or in any

way processed by an organization, the hardware and software that constitutes the configuration of computer systems, a social system that is formed by the actions and relations among the IS users, as well as a set of procedures that guide the users' actions. Under this perspective, IS have not only a technical part, but also a social dimension. IS are of high significance to organizations across a wide range of economic sectors. In consequence, their proper function and unobstructed operation is a critical issue that has attracted the attention of both IS research and practice. Information systems security management is a stream of management activities that aim to protect the IS and create a framework within which the IS operates as expected by the organization.

2.0 What is SISP?

IS/IT planning is the organized planning of IT infrastructure and applications portfolios done at various level of organization. It is very important to both user and planner because end user do IS/IT planning for their own units; end user must participate in the corporate planning, therefore they must understand the process; corporate planning determines how the IS/IT look like and determine what applications end user can deploy. Finally the future of every unit in the organization will be impacted by the IS/IT infrastructure.

SISP is the process of identifying a portfolio of computer-based applications to serve an organization best. Ideally, the organization makes SISP part of its strategic business planning process to link the resulting IT strategy to the business strategy. SISP also includes the specification of databases and systems to support those applications. SISP may encompass the selection of conventional applications that best fill the organization's current and future needs. SISP also may entail the search for new applications with the potential to create an advantage over competitors.

To perform SISP, an organization usually carries out a major, intensive study. Most follow one of several, similar well-defined and documented methodologies; a few spend the time on their own versions. Committees of users and IS specialists are more common, often using the methodology's vendor for training and guidance. During the multi-steps study, a portfolio of applications is defined, along with appropriate priorities, databases, data elements, and a network of computers and communications equipment to support them. The study also provides a schedule for their development and installation. The organization periodically updates the plan after its initial approval.

SISP basically address four general issues; aligning IS/IT plan with the organizational business plan; designing IS/IT architecture for organization in such a way that user, applications and databases can be integrated and network together; efficiently allocating information systems development and operational resource among competing applications and finally planning information project in order to complete on time and within budget and include the specific functionalities.

3.0 The Perspective of Strategic Information Systems Planning

In order to put the planning for strategic information systems in perspective, the evolution of information systems according to the three-era model of John Ward, et al.(1990) is pertinent. According to this model there are three distinct, albeit overlapping, eras of information systems, dating back to the 60's. The relationship over time of the three eras of information systems is shown in table 1 below:

Table 1: The Three Era Model of IS (Ward, 1996)

	ERA	CHARACTERISTICS
60s	Data Processing DP)	Standalone computers, remote from users, cost reduction function.
70s &80s	Management Information Systems (MIS)	Distributed process, interconnected, regulated by management service, supporting the business, user driven.
80s &90s	Strategic Information Systems (SIS)	Networked, integrated systems, available and supportive to users, relate to business strategy, enable the business - business driven.

Applications in the overall Data Processing (DP), Management Information Systems (MIS) and Strategic Information Systems (SIS) area need to be planned and managed according to their existing and future contribution to the business. Traditional portfolio models consider the relationship of systems to each other and the tasks being performed rather than the relationship with business success. A portfolio model derived from McFarlan (1984) considers the contribution of IS/IT to the business now and in the future based on its industry impact. Based on this model applications are divided into four categories, as shown in table 2 below.

Table 2: A Portfolio Model (McFarlan, 1984)

Strategic (Applications which are critical for future success. Examples: computer-integrated manufacturing, links to suppliers, etc.)	**Turnaround** (Applications which may be of future strategic importance. Examples: electronic data interchange with wholesalers, electronic mail, etc.) manufacturing, links to suppliers, etc.)
Factory (Applications which are critical to sustaining existing business. Examples: employee database, maintenance scheduling, etc.)	**Support** (Applications which improve management and performance but are not critical to the business. Examples: time recording, payroll, etc)

4.0 Strategic Information Systems Planning Methodology

The task of strategic information systems planning is difficult and often organizations didn't know how to do it. Strategic information systems planning is a major change for most organizations, from planning for information systems based on users' demands to those based on business strategy. Strategic information systems planning can changes the planning characteristics in major ways. For example, the time horizon for planning changes from 1 year to 3 years or more and development plans are driven by current and future business needs rather than incremental user needs. Increase in the time horizon is a factor which results in poor response from the top management to the strategic information systems planning process as it is difficult to hold their attention for such a long period.

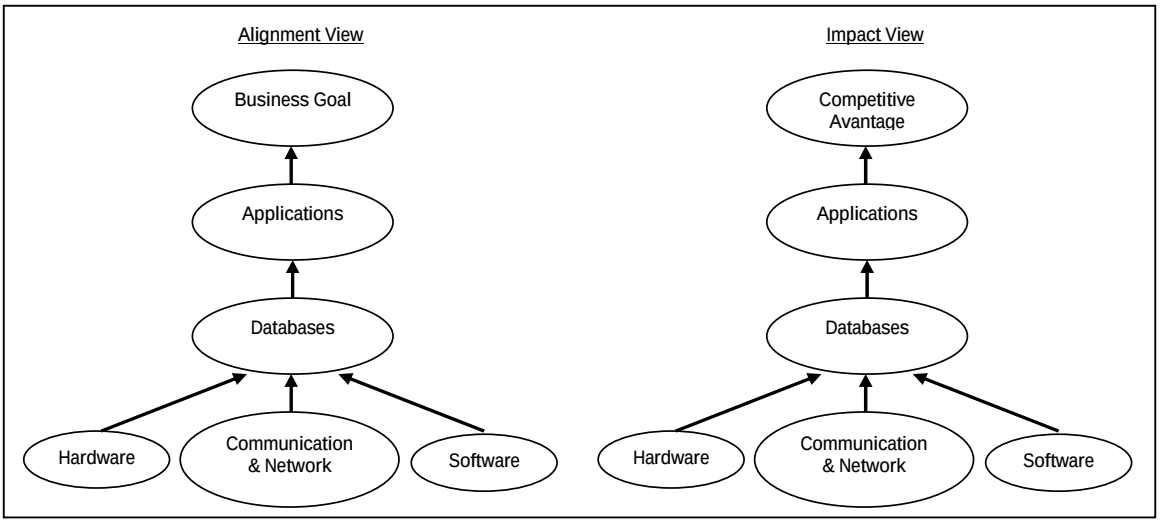

Figure 1.0 Two Views of SISP Methodologies (Pant, 1995)

Other questions associated with strategic information systems planning are related to the scope of the planning study, the focus of the planning exercise - corporate organization vs. strategic business unit, number of studies and their sequence, choosing a strategic information systems planning methodology or developing one if none is suitable, targets of planning process and deliverables. Because of the complexity of the strategic information systems planning process and uniqueness of each organization,

there is no one best way to tackle it. classify SISP methodologies into two categories: *impact* and *alignment* (Vitale, et al. 1986). Impact methodologies help create and justify new uses of IT, while the methodologies in the “alignment” category align IS objectives with organizational goals. These two views of SISP are shown in figure 1.0 above.

4.1 The Strategic IS/IT Planning Process

The planning process in strategic IS/IT planning consist input, output and processing activities (Ward, 1996). Figure 3 shows the input and outputs of the planning process.

The input activities are internal business environment, external business environment, internal IS/IT environment, and external IS/IT environment. Internal business environment is the current business strategy, objective, resources, processes and the culture and values of the business. External business environment are the economic, industrial and competitive climate in which the organization operates. Internal IS/IT environment is the current IS/IT perspective in the business, its maturity, business coverage and contribution, skills, resources and technological infrastructure. The current application portfolio of existing systems and systems under development, or budgeted but not yet under way also part of the internal IS/IT environment. External IS/IT environment is the technology trend and opportunities and the use made of IS/IT by external bodies.

The output activities are IS/IT management strategy, business IS strategy and IT strategy. IS/IT management strategy is the common elements of the strategy that apply throughout the organization, ensuring consistent policies where needed. Business strategy is how each unit or function will deploy IS/IT in achieving its business objectives. Alongside each of these are application portfolios to developed for the business unit and business models describing the information architecture of each unit. The portfolios may include how IS/IT will be used at some future date, to help the units to achieve their objective. IT strategy is a policy and strategies for the management of technology and specialist resources.

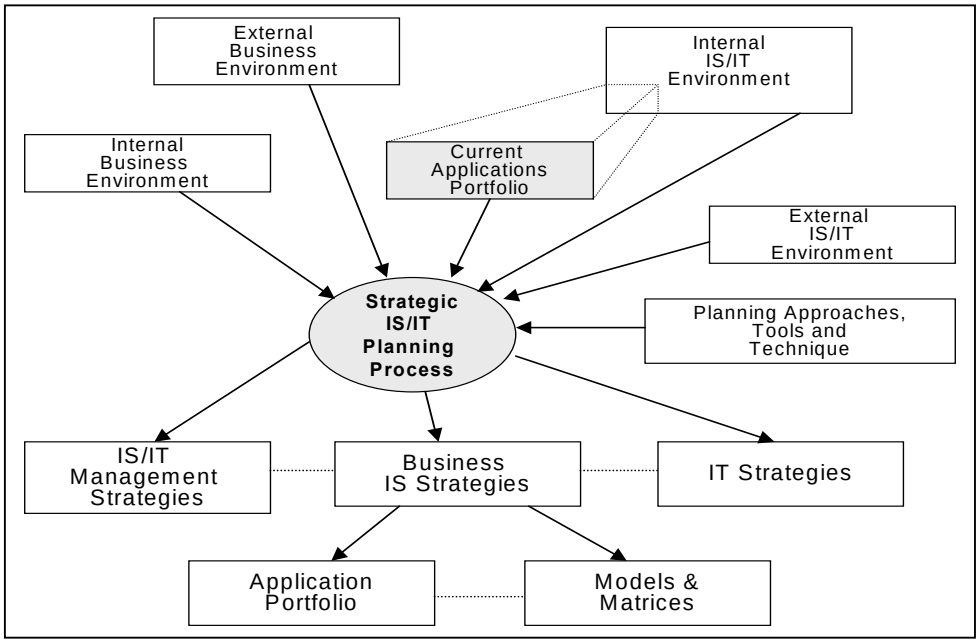

Figure 2.0 The inputs and outputs of the planning process (Ward, 1996)

6.0 What is successful SISP?

The objectives of SISP may include aligning IT with the business, gaining competitive advantage, identifying new and higher payback applications, identifying strategic applications, increasing top management commitment, improving communications with users, forecasting IT resource requirements, allocating IT resources, developing an information architecture, and increasing the visibility of IT. The extent SISP fulfills these key objectives for an organization offers a way to assess SISP success. A comprehensive review of the recent IS planning literature reveals that the following factors are related to the success of the IS planning process:

- the need to align the corporate objectives with the IS strategy
- the underlying motivation for the initialization of the planning process
- the level of maturity of the organization
- the methodology used in developing the IS plan
- the framework used for setting IT investment priorities
- the measurement of effectiveness used for the IS department
- preparation of an implementation plan is critical to meeting SISP objectives

Although these individual success factors have enjoyed much discussion, there have been few empirical attempts to relate actual success of a SISP project to the detailed activities, techniques and processes which contributed to that project.

7.0 Information Security Defined

Information security defined as an information security program that plan to mitigate risk associated with the processing of information in three element which defined by security professional (Wlyde, 2004):

- **Confidentiality.** The prevention of unauthorized use or disclose of information. Privacy is closely related topic that has lately been getting more and more visibility
- **Integrity.** Ensuring that information is accurate, complete, and has not been modified by unauthorized user or process.
- **Availability.** Ensuring that the users have timely and reliable access to their information assets.

These three elements (CIA) are the basics around which all security programs are developed. Both of them are linked together in the idea of information protection. The main idea is to show that information is an asset that requires protection.

7.1 Information Security Domains

There are ten main domain of information security that made up the Common Body of Knowledge (CBK) maintained by the International Information Security Certification Consortium (ISC^2) as followed:

- *Assess control systems and methodology.* These core application systems that people think of when discussing information security. This area address the use of information systems and how to manage and restrict access to the system or application

- *Telecommunication and network security.* Similar to first domain, but address issues regarding transmission of information and transport mechanisms; networks and connectivity
- *Security management practice.* This domain addresses policies and management practice, including risk management.
- *Application and systems development security.* This domain deals with the development life cycle (SDLC) and data management from and information security perspective.
- *Cryptography.* These domain cover the principles and methods use to protect information through the use of codes and secrecy
- *Security architecture and models.* This domain covered the design and architecture of computers and networks and how to protect them.
- *Operations security.* This domain address the control involve in the operation of data center, and the management issues resulting from applications as they are used in the business environment.
- *Business continuity planning (BCP) and disaster recovery planning (DRP).* This domain cover the policies and procedures need to ensure that business protects information resources from the effects of systems failures and outages.
- *Laws, investigation, and ethics.* This domain covers the legal and ethical issues for business
- *Physical security.* This domain covers the physical security measures that are involved in protecting the assets of the company.

8.0 Overview of the Computer System Life Cycle

There are many models for the computer system life cycle but most contain five basic phases as shown in figure 3.0 and the IT security in Table 3.0:

- *Initiation*. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.
- *Development/Acquisition*. During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.
- *Implementation*. After initial system testing, the system is installed or fielded.
- *Operation/Maintenance*. During this phase the system performs its work. The system is almost always modified by the addition of hardware and software and by numerous other events.
- *Disposal*. The computer system is disposed of once the transition to a new computer system is completed.

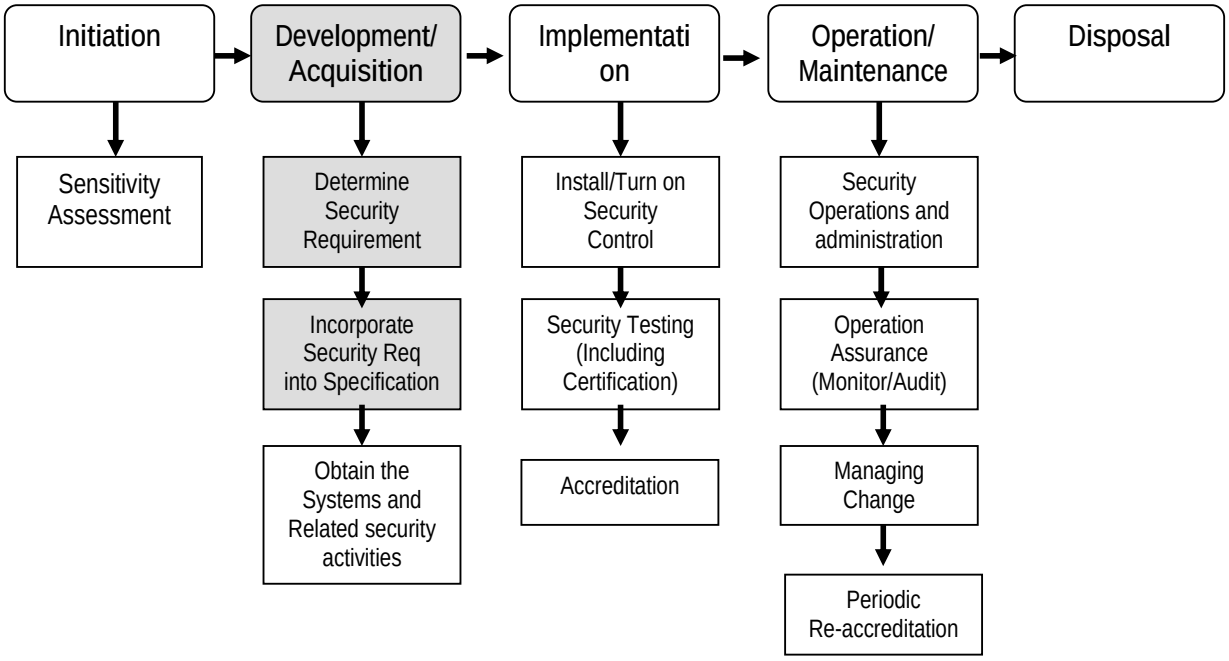

Figure 3.0 Security In System Life Cycle (NIST)

Table 3.0 IT Security in the SDLC(Grance, 2004)

	Initiation	Development/ Acquisition	Implementation	Operational/ Maintenance	Disposal
SDLC	- Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternatives to Capital Assets • Preparing for investment review	Functional Statement of Need - Market Research - Feasibility Study - Requirements Analysis - Alternatives Analysis - Cost-Benefit Analysis - Software Conversion Study - Cost Analysis - Risk Management / Plan - Acquisition Planning	Installation - Inspection - Acceptance testing - Initial user training - Documentation	Performance measurement - Contract modifications - Operations - Maintenance	- Appropriateness of disposal - Exchange and sale - Internal organization screening - Transfer and donation - Contract closeout
SECURITY CONSIDERTIONS	- Security Categorization - Preliminary Risk Assessment	- Risk Assessment - Security Functional Requirements Analysis - Security Assurance Requirements Analysis - Cost Considerations and Reporting - Security Planning - Security Control Development - Developmental Security Test and Evaluation - Other Planning Components	- Inspection and Acceptance - System Integration - Security Certification - Security Accreditation	- Configuration Management and Control - Continuous Monitoring	- Information Preservation - Media Sanitization - Hardware

9.0 Benefits of Integrating Security in the Computer System Life Cycle

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. Security, like other aspects of a computer system, is best managed if planned for throughout the computer system life cycle. It has long been a tenet of the computer community that it costs ten times more to add a feature in a system *after* it has been designed than to include the feature in the system at the initial design phase. The principal reason for implementing security during a system's development is that it is more difficult to implement it later (as is usually reflected in the higher costs of doing so). It also tends to disrupt ongoing operations. Security also needs to be

incorporated into the later phases of the computer system life cycle to help ensure that security keeps up with changes in the system's environment, technology, procedures, and personnel. It also ensures that security is considered in system upgrades, including the purchase of new components or the design of new modules. Adding new security controls to a system after a security breach, mishap, or audit can lead to haphazard security that can be more expensive and less effective that security that is already integrated into the system. It can also significantly degrade system performance. Of course, it is virtually impossible to anticipate the whole array of problems that may arise during a system's lifetime. Therefore, it is generally useful to update the computer security plan at least at the end of each phase in the life cycle and after each re-accreditation. For many systems, it may be useful to update the plan more often. Life cycle management also helps document security-relevant decisions, in addition to helping assure management that security is fully considered in all phases. This documentation benefits system management officials as well as oversight and independent audit groups. System management personnel use documentation as a self-check and reminder of why decisions were made so that the impact of changes in the environment can be more easily assessed. Oversight and independent audit groups use the documentation in their reviews to verify that system management has done an adequate job and to highlight areas where security may have been overlooked. This includes examining whether the documentation accurately reflects how the system is actually being operated.

10.0 Integrating the Strategic IS/IT Planning with Information Security

Integrating both Strategic IS/IT planning process with the Information Security Domain as define in 5.1 will produce more valuable SISP to the organization. The appropriate domain should include in the SISP process as an input in the external business environment, external IS/IT environment, internal business environment and internal business environment. As for example, security management practice domain should

include in all input attributes; security management in internal and external business and IS/IT environment. Beside SISP and Information Security Domain, Computer System Life Cycle as describe at 6.0 above should be incorporate in the establishment of SISP, especially in the development/acquisition phase. At this phase, security requirement was identified then incorporate security requirement into specification.

11. Conclusion

Embedding Information Security Domain in the Strategic IS/IT Planning is an idea to increase the capability of SISP outcome. The deliverable from the SISP process will more beneficial to the organization especially to the IS/IT department. Most of the problem will occur on the implementation and operational of the information system in the organization. Although the organization will face a security problem in the implementation and operational phase, they can add value to the security components rather than restart the security planning from the beginning.

Reference

An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce. Special Publication 800-12

British Standard BS 7799-1: 1999; Information Security Management, BSI/DISC Committee BDD/2, 1999, www.bspsl.com/secure/iso17799software/cvm.cfm

Doherthy, N. F., Marples, C. G. & Suhaimi A. (1999), The relative success of alternative approaches to strategic information systems planning: an empirical analysis, Journal of Strategic Information Systems. Vol 8 pp 263-283.

Earl, M. J. (1993), *"Experience in strategic information systems planning"*. MIS Quaterly Mac, pp1-24.

Grance, T., Hash, T. & Stevens, M. (2004). Security Considerations in the Information System Development Life NIST Special Publication 00 64 REV.

Greene, F. (2002). A Survey of Application Security in Current International Standards, Information Systems Control Journal, Volume 6, 2002.

Hevner, A. R., Berndt D. J. & Studnicki J. (2000). *"Strategic information systems planning with box structures".* IEEE Proceeding of the 33rd Hawaii International Conference on Systems Science. Hawaii, January 2000.

King, W. (1995). Creating A Strategic Capabilities Architecture, Information Systems Management, v.12.

Krause, M. & Tipton, H. F. (1999). Handbook of Information Security Management. Auerbach Publications Inc.

Lederer, A., L., Sethi, V. (1998). Seven Guidelines For Strategic Information Systems Planning, Information Strategy: The Executive's Journal, 07438613, Fall98, Vol. 15, Issue 1, p23, 6p, Auerbach Publications Inc.

McFarlan, F. W. (1984). Information Technology Changes The Way You Compete, Havard Business Review, May-Jun 1984, pp. 98-105

Pant, S. & Hsu, C. (1995). Strategic Information Systems Planning: A Review. Information Resource Management Association International Conference, May 21-24, Atlanta, Georgia.

Tipton, H. F. & Krause, M. (2002). Information Security Management Handbook, 4th Edition, Auerbach Publications Inc.

Turban, E., Mclean, E., & Wetherbe, J. C. (2002). Information Technology For Management: Transforming Business In The Digital Economy, 3rd Edition, John Willey & Sons, Inc.

Vitale, M., Ives, B. & Beath, C. (1986). Identifying trategic Information Systems, Proceeding 7th international Conference on Information Systems, San Diego. Pp265-276.

Ward, J. & Griffith, P. (1996).Strategic Planning For Information Systems (2nd Edition).John Wiley & Son, London.

Wylder, J. (2004).Strategic Information Security, Auerbach Publication,